Risk Assessment
For

Authentication Infrastructure, KDC
[ID#]

Prepared by: Ray Stefanski **Date:** 9/1/05
MiniBooNE Computer Coordinator

Approved by: Chris Green **Date:** 9/1/05
MiniBooNE Computer Operations

Approved by: Amber Boenhlein **Date** 9/1/05
System Administrator

Approved by: Jason Heddon **Date:** 9/1/05
GCSC

Approved by: Richard Van deWater **Date:** 9/1/05
System/Application Owner

Approved by: Steve Brice **Date:** 9/1/05
System/Application Owner

Approved by: Victoria White **Date:** 9/1/05
Division Head

1. SYSTEM IDENTIFICATION

1.1. System Name/Title

Fermilab Identifier E-898/944 - MiniBooNE.(MiniBooster Neutrino Experiment) has been assigned to the system discussed throughout this risk assessment and will be referred to as the MiniBoone data acquisition, storage and monitoring system.

1.2. System Type

Experiment data acquisition, storage and control.

1.3. OMB 53 Exhibit Information

the MiniBoone data acquisition, storage and monitoring system is discussed and defined in the Memorandum of Understanding between E-944 and the Computing Division.

1.4. Responsible Organization

Fermi National Accelerator Laboratory
PO Box 500
Batavia, IL 60510

1.5. Information and Security Contact(s)

Security contacts are established in the MiniBooNE MOU with the Computing Division, and are given in table 1. The system manager is registered in the MISCOMP database. The GCSC is identified at http://computing.fnal.gov/security/contacts.html

Table 1, security contacts:

Title	Name	Email	Telephone
MA Coordinator	Richard Van deWater	vdwater@fnal.gov	630.840.2092
System Manager	Amber. Boehnlein	cope@fnal.gov	630-879-5105
GCSC	Jason Hedden	jhedden@fnal.gov	630-840-6669
Physical Key Holder	MBCR Operator MCR Crew Chief	www-boone.fnal.gov www-bd.fnal.gov	630.840.2757 630.840.3721
System/Application Owner	Steve Brice	sbrice@fnal.gov	630.840.8748

1.6. System Operational Status

The MiniBoone data acquisition, storage and monitoring system is in the Operational phase of its life-cycle.

1.7. Information Gathering Technique

This assessment was carried out by the preparer, and vetted with document review by system experts.

1.8. General Description/Purpose

This system provides for data acquisition, storage and monitoring for MiniBooNE.

1.8.1. Introduction

MinibooNE is a neutrino experiment that runs in the Booster Neutrino Beam – a facility roughly consisting of a target to produce secondary particles, and a magnetic horn to focus the beam to a detector that resides at the MiniBooNE detector building (MDB).

1.9. System Description and Boundaries

MiniBooNE is run from a control room located in WH10W, where operators observe and monitor the beam, horn and detector. Control and operation of the proton beam and horn are in the hands of the Main Control Room operators, who rely on the MiniBooNE operators to bring problems to their attention. We can think of operations in two parts: control or, more accurately, monitoring of the beam and experiment, and data acquisition, which requires high bandwidth transfer of information from the beam and detector to the data storage center at the FCC. A third component of the system involves data storage in the Enstore facility at the FCC. MiniBooNE also uses seven terabyte servers for storage of processed data and simulated events. The computers involved in monitoring, data acquisition and data storage are listed in table 2.

Table 2: List of computers in the MiniBooNE DAQ, data storage and monitoring systems.

Type	System Name	Operating System	Purpose	Location	Owner	Machine Class
DAQ	hal9000	6.2	Main DAQ on private net.	MBD	fermilab	VALINUX: 2230
DAQ	southport	SL303	Replacement for hal9000	MBD	fermilab	POLYWELL: 935X4A
DAQ	hal9002	7.3.2	Main DAQ	MBD	indiana	PENGUIN: REL110-D-P3-1000-RM
DAQ	hal9004	7.3.2	Main DAQ	MBD	indiana	PENGUIN: REL110-D-P3-1000-RM
DAQ	damen	7.3.2	BNB ACNET DAQ	MBD	lanl	Dell: OptiPlex GX150
DAQr	division	7.3.2	NuMI ACNET DAQ/Bull's Eye DAQ	MBD	columbia	Dell: OptiPlex GX240
Console-server	booneterm		Console-server at MBD	MDB		XYPLEX TERMINAL SERVER
DAQ	dorchester	7.3.2	LMC DAQ	MI13A	colorado	DELL: PowerEdge 2650
DAQ	walcott	7.1.1	RWM DAQ	MI12	lanl	Dell: Dimension XPS
Monitor	colfax	3.05	MBCR detector monitor	WH1050	colorado	Dell Precision WorkStation 370
Monitor	cns22pc	WXP	MBCR beam monitor	WH1050	AD	Gateway: E4200-800P3
DB Server	wacker	7.3.2	DB server	WH1073	lanl	Dell Precision WorkStation 340
Monitor	hotspur	W2000	Horn DAQ	MI12	fermilab	DELL-XPS-T800-MT
Controller	Laser PC	W	Laser Calibration System	MBD	LSU	Gateway E4200 500
Monitor	magnolia	3.04	On-line event display/Booster Monitor.	WH1050	fermilab	Dell Precision WorkStation 650
NIS Server	maxwell	7.3.2	Condor pool manager; runs BB.	WH1073	michigan	Dell Precision WorkStation 340

Data Storager	mbdata02	SL 304	Terabyte Servers	FCC/2/218	fermilab	POLYWELL: 2*3.06G-Xeon,4U-RM
Data Storage	mbdata01	SL 304	Terabyte Servers	FCC/2/218	fermilab	POLYWELL: 2*3.06G-Xeon,4U-RM
Data Storage	lake	SL 303	Terabyte Servers	FCC/2/218	fermilab	POLYWELL: 2*3.06G,4U-RM
Data Storage	bishopford	3.01	Terabyte Servers	FCC/2/218	fermilab	KOI: PLY-935X8
Data Storage	edens	3.01	Terabyte Servers	FCC/2/218	lanl	POLY 935X8
Data Storage	kingery	3.01	Terabyte Servers	FCC/2/218	princeton	POLYWELL: 2*X-2.4G-3.8T-5U-RM
Data Storage	Dan ryan	7.3.2	Terabyte Servers	WH1052	michigan	POLY 935X8
Console-server	cicero		Console-server at FCC	FCC/2/218	fermilab	CYCLADES: ACS32

The boundary of the MiniBoone data acquisition, storage and monitoring system is at its network interface which connects the devices in Table 2 to the General Computing Enclave.

1.10. Information Sensitivity

The data sensitivity on the MiniBoone data acquisition, storage and monitoring system is classified in the following table:

Relative Importance of Protection Needs			
	HIGH (Critical Concern)	MEDIUM (Important Concern)	LOW (Minimum Concern)
Confidentiality			X
Integrity			X
Availability			X

The information available in the MiniBooNE data acquisition, storage and monitoring system is relevant only to the physicists using the data. It has no relevance beyond the basic science carried out by the experiment.

2. Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised.

2.1. Threat Source Identification

There are no threat sources which have not been identified in the Risk Assessment for the General Computing Enclave.

2.2. Motivation and Threat Actions

There are no motivations and threat actions which have not been identified in the Risk Assessment for the General Computing Enclave.

3. Vulnerability Identification

MiniBooNE protects data from corruption from any one of several sources:

a. Misuse of the MiniBooNE cluster by user's from beyond the firewall, by adhering to the practices specified by for General Computing Enclave.
b. Misuse of the MiniBooNE cluster by user's from inside the firewall, by adhering to the practices specified by for General Computing Enclave.
c. .Loss of data due to operator failure is not likely, because no operator intervention is required in the data acquisition, storage or monitoring process.
d. Corruption of data during analysis is not likely, because data cannot be written into Enstore by a data analyzer. Only the Data Acquisition computer, Hal9002/4, can write into Enstore. There is no other mode available to write to Enstore. Maintenance of data quality in Enstore is part of the CD operational responsibilities.

e. Loss of data due to equipment failure.
f. Loss of data acquisition opportunities by running the experiment due to equipment failure.
g. Loss of processed data due to equipment failure.
h. Loss of processed data due to failure on the part of the person processing data.

4. Control Analysis

Mitigation of vulnerabilities a, b, c, and d, are part of the procedures for the General Computing Enclave, and no additional mitigation is done specific to the MiniBooNE data acquisition, storage and monitoring system. The following controls specific to MiniBooNE and are in place to mitigate the following vulnerabilities:

Mitigation 1: Data is stored in a buffer (Hal9002/4) as the experiment is run. From the buffer it is transmitted to Enstore. The buffer is sufficiently large to store several days of normal data acquisition. This has proven to be adequate protection against a failure in the Enstore system, and no data loss has occurred due to this vulnerability.

Furthermore, the main data acquisition computers (Hal9000/2/4) and local data storage are kept in climate controlled racks, and have uninterruptable power sources. It's known that power cycling can shorten equipment lifetime, so this equipment is never turned off. There has never been a loss of operational time due to failure of the main DAQ or the local data storage units.

Mitigation 2: MiniBooNE has an operating efficiency of 99%, which is excellent for accelerator based experiments. Loss of running time does occur whenever there is a failure in any of the DAQ computers listed in Table 2. Rapid recovery depends on various factors:

1. The standard Fermilab Linux operating system is mounted on each computer, wherever possible. This provides the computers with the latest updates through the yum facility.
2. Computer applications and in-house code is stored in CVS for easy retrieval.
3. The experiment runs a backup system for the critical DAQ machines.
4. The experiment keeps a sufficient number of spares to replace any failures quickly.

Mitigation 3: Processed data and simulations are stored in the Terabyte servers. The servers are RAID arrays of about ten hard-drives apiece. A single server can hold several terabytes of data. The server could lose an entire store of data if two of the hard drives in the set fail simultaneously, since that causes the server to lose control of the array. Mitigation involves:

1. Maintaining at least two spare hard drives for each server.

2. Monitoring the servers with the Big Brother monitoring system. CD personnel are ready to replace a failed drive typically within 24 hours, including weekends and holidays.

There has never been a loss of a full array of data in a terabyte server.

Mitigation 4: Individuals that write applications and process data for MiniBooNE, are responsible for protecting their data by using CVS or by taking advantage of appropriate backup opportunities.

5. Likelihood Determination, Impact Analysis, and Risk Level

Risk is related to the likelihood of a successful exploit of vulnerability, and the related impact. We use Table3 to define risk and the dependence of risk on likelihood and impact.

Table 3: Risk Analysis:

Threat Likelihood	Impact		
	Low	Medium	High
Low	Low	Low	Low
Medium	Low	Medium	Medium
High	Low	Medium	High

5.1 Loss of data due to equipment failure.

The risk of loss of data due to equipment failure is low, because the data are buffered, the DAQ equipment is maintained for minimum failure, and the amount of data transmitted to Enstore is a small portion of the total data collected by the experiment.

5.2 Loss of data acquisition opportunities by running the experiment due to equipment failure.

The risk of loss of data acquisition opportunities due to equipment failure is low, because the collaboration operates the experiment in a way that supports quick recovery from failure. The fact that the experiment has a 99% up-time demonstrates this point.

5.3 Loss of processed data due to equipment failure.

The loss of data stored in a terabyte server would have an important impact on the experiment. However, only process data and simulations are stored in the servers, and these could be reprocessed or rerun if necessary. Furthermore, the probability of such a failure is very low. Therefore the risk for loss of data due to this source is low.

5.4 Loss of processed data due to failure on the part of the person processing data.

The highly capable and professional people working on MiniBooNE will make this risk extremely small.

6. Control Recommendations

The only threat likelihood which is not low is how the individual user's credentials are handled. Since this is outside the control and scope of the data acquisition, storage and monitoring system, no additional controls are recommended at this time.

7. Risk Mitigation

No additional mitigation action is planned at this time and the risk levels identified above are accepted.